SC-RS5FJ

取 扱 説 明 書

http://www.sun-denshi.co.jp/sc/

目次

はじめに

この度は「Rooster-RW」SC-RS5FJをご購入いただき誠にありがとうございました。本取扱説明書はRoosterーRWを正しくご使用いただくために必要な操作方法、機能について記述してあります。お使いになる前に必ずお読みください。

Rooster-RWはFOMA、AIR-EDGE、b-mobile、CDMA 1X WIN、ソフトバンクコネクトカード等のモバイルデータ通信カード（以後、モバイルカード）及びブロードバンドに対応した多機能アクセスルータです。
モバイルカードをRooster-RWに接続することにより、㈱ウィルコムや㈱NTTドコモが提供する低コストワイヤレスデータ通信サービスを利用し、複数のパソコンからインターネットアクセスが可能となります。
更に、㈱ウィルコムが提供するPUSH型情報配信システム「WakeOnサービス」に対応する「WakeOn機能」をルータとしては初めて搭載するとともに、携帯電話等からの着信をトリガとして自動的にダイヤルアップする「WakeOn Voice機能」、㈱NTTドコモが法人市場向けに提供しております「FOMAによるLAN接続サービス」に対応した「FOMA LAN着信機能」、ネットワークカメラやASPサービスなどとの連携を容易にする「アドレス解決機能」、モバイルカードによりインターネットを経由せず直接ローカルのネットワークへアクセスする事を可能にする「リモートアクセス機能」等、モバイル環境でのシステム構築に最適な高性能ゲートウェイ機能を搭載しております。

同梱品の確認

パッケージには、次のものが同梱されています。万一不足しているものがありましたら、お買い求めの販売店、もしくはサポートセンターにご連絡ください。

● Rooster-RW　SC-RS5FJ （本体） 1 台

● AC アダプタ　1 個

● UTPケーブル（カテゴリー5ストレート） 1 本

●縦置きスタンド　1 個

●マニュアル、書類
取扱説明書（CD-ROM）　1 枚
保証書　1 通

この取扱説明書について

表記について

●マークの意味

本取扱説明書では、安全にお使いいただくために、守っていただきたい事項に次のマークを表示しています。

	人体に危険を及ぼしたり、装置に大きなダメージを与える可能性があることを示しています。必ずお守りください。
	機能停止を招いたり、各種データを消してしまう可能性があることを示しています。十分に注意してください。
メモ	関連情報です。参考にお読みください。

●略称について

本取扱説明書ではRooster　SC-RS5FJのことを本製品、Microsoft WindowsをWindows、10BASE-T/100BASE-TXケーブルのことをUTPケーブルと表記しています。
また、パソコンから本製品へファイルを転送（コピー）することをアップロード、本製品からパソコンへファイルを転送（コピー）することをダウンロードと表記しています。

●設定例について

本取扱説明書に記載されているIPアドレスやドメイン名、URLアドレスなどの設定例は、説明のためのものです。実際に設定するときには、必ずご使用の環境に合わせて読み替えてください。

商標について

■「FOMA」は株式会社NTTドコモの登録商標です。
■「AIR-EDGE」は株式会社ウィルコムの登録商標です。
■「b-mobile」は日本通信株式会社の登録商標です。
■「どこでもカメラ」はヴイ・インターネットオペレーション株式会社の登録商標です。
■「Rooster」「SunCommunications」はサン電子株式会社の登録商標及び、商標登録出願中です。
■Apple、Macintosh、MacOSは米国Apple社の登録商標及び商標です。
■Microsoft、Windows、InternetExplorerは米国Microsoft社の米国及びその他の国における登録商標です。
■その他、本取扱説明書に記載されている会社名、製品名は、各社の商標または登録商標です。本文中の各社の登録商標または商標には、TM、Ⓡマークは表示しておりません。

安全にお使いいただくために

ここに記載している事項は、安全に関わる重要な内容ですので、必ず守ってください。本取扱説明書では、安全上の注意事項を「警告」と「注意」に区分しています。

⚠警告	この表示を無視して、間違った取り扱いをした場合、人が死亡または重傷を負う可能性が想定される内容を示しています。
⚠注意	この表示を無視して、間違った取り扱いをした場合、人が損害を負う可能性が想定される内容、および物的損害のみの発生が想定される内容を示しています。物的損害とは、家屋、家財および家畜、ペットに関わる拡大損害を示しています。
⃠	禁止行為（してはいけないこと）を示しています。
❗	強制行為（必ずしなければいけないこと）を示しています。

なお、注意、禁止に記載した事項でも、状況によっては重大な結果に結びつく場合があります。いずれも重要な内容を記載していますので、必ず守ってください。

⚠注意

分解禁止

本製品を分解したり、改造したりしないでください。
● 感電、火災、故障の原因になります。

禁止

雷のときは、本製品およびケーブルに触れないでください。
● 感電の原因になります。

禁止

本製品に水などの液体をかけたり、異物を入れないでください。
● 感電や火災の原因になります。万一、本製品に液体がかかったり、異物が入った場合は、AC アダプタをコンセントから抜いて、点検修理を依頼してください。

強制

本製品から煙、異臭、異常音が発生した場合は、AC アダプタをコンセントから抜き、本製品を接続している機器からケーブルを取り外してください。また、修理、点検を依頼してください。
● 火災の原因になります。

禁止

この取扱説明書に記載されている周囲環境条件以外では、使用、保管しないでください。

●本製品の故障や破損などによって、発煙、発火、感電の原因になります。
　下記の環境には、特にご注意ください。
●室内または製品周囲の温度や湿度が極端に高い、または低い場所
●結露がある場所
●急激な温度変化が起きる場所
●ほこりが多い場所
●静電気が発生しやすい場所
●腐食性のガスが発生する場所
●水などがかかりやすい場所
●振動や衝撃が加わるような不安定な場所
●油煙が当たる場所
●直射日光が当たる場所
●製品周囲に発熱する器具や燃えやすい物がある場所
●周囲に置いてある物との間に適切な空間がない場所

禁止

同梱の AC アダプタ以外の AC アダプタを使用しないでください。

●他の AC アダプタを使用すると、故障、火災の原因になります。

禁止

電源ケーブルを傷つけないでください。

●感電、火災の原因になります。

強制

AC アダプタは、AC100V コンセントに接続してください。また、本製品を設置、移動するときは、電源プラグを抜いてください。

●火災や感電の原因になります。

禁止

梱包のポリ袋などは、小さいお子様の手の届くところに置かないでください。

●小さいお子様がかぶったり、飲みこんだりすると、呼吸を妨げる危険があります。

強制

60cm 以上の高さから落とした場合は、使用を中止し、点検、修理を依頼してください。

●そのまま使用すると、重大な事故につながる可能性があります。

強制

電源プラグは確実に根元まで差し込んでください。また、電源プラグとコンセントの間のほこりは、定期的（半年に 1 回程度）に取り除いてください。

●電源プラグの間にほこりが付着し、電源が短絡して発煙、発火、火災の恐れがあります。

ご使用にあたってのお願い

本製品周辺で静電気的障害を発生させないでください。

●本製品は、静電気に敏感な部品を使用しています。特に、コネクタの接点、ポート、その他の部品に、素手で触れないでください。部品が静電破壊するおそれがあります。

本製品はていねいに取り扱ってください。

●本製品に強いショックを与えると破損の原因になります。

本製品のお手入れは、電源を切った状態で行ってください。

●誤動作や故障の原因になります。

本製品のお手入れには、揮発性の有機溶剤、薬品、化学ぞうきんなどを使用せず、乾いた柔らかい布で拭いてください。汚れがひどい場合は、柔らかい布に台所用中性洗剤をしみこませて固く絞ってから拭き、最後に乾いた柔らかい布で仕上げてください。

●揮発性の有機溶剤、薬品、化学ぞうきんなどを使用すると、変質、変色、場合によっては破損の原因になります。

地球環境保全のため、次のことにご協力ください。

●本製品および付属品は、不燃物として処分してください。
●廃棄方法は、地方自治体などで決められた分別収集方法に従ってください。
●一般ごみとして、家庭で焼却処分しないでください。ダイオキシンや塩化水素ガスなどが発生し、環境や人体に影響を与えます。

ご注意

本製品の使用は国内向けになっておりますので、海外ではご利用になれません。
These products are designed for use in Japan only and cannot be used in any other countries.

本製品は、パソコンなどのOA機器に使用することを目的に設計、製造されています。医療機器や幹線通信機器、電算機システムなどの、極めて高い安全性や信頼性が要求される用途には使用しないでください。

取扱説明書について、次の点にご注意ください。

(1) 本取扱説明書の内容の一部または全部を、無断で転載することを禁止します。
(2) 本取扱説明書の内容に関しては、将来予告なしに変更される場合があります。
(3) 本取扱説明書の内容については、万全を期して作成いたしましたが、万一ご不審な点やご不明な点、誤り、記載漏れ、乱丁、落丁、その他お気づきの点がございましたら、当社までご連絡ください。
(4) 適用した結果の影響につきましては、(3) 項にかかわらず責任を負いかねますので、ご了承ください。
(5) 本取扱説明書内で指示されている内容には、必ず従ってください。本取扱説明書に記載されている内容を無視した行為や誤った操作によって生じた障害や損害については、保証期間内であっても責任を負いかねますので、ご了承ください。

この製品について

本製品は、FOMA、AIR-EDGE、b-mobile等のモバイルデータ通信カード及び
ブロードバンドに対応した多機能アクセスルータです。

主な特徴

●各社モバイルカードに対応

㈱NTTドコモが提供する「FOMA」、㈱ウィルコムが提供する「AIR-EDGE」、日本通信㈱が提供する「b-mobile」、KDDI㈱が提供する「CDMA 1X WIN」、ソフトバンクモバイル㈱が提供する「コネクトカード」など各社モバイルカードを接続することにより、1回線の契約のみで本製品に接続された複数台のパソコンから同時にインターネットアクセスが可能となります。

● WakeOn 機能を搭載

WakeOnサービス対応のAIR-EDGEカードをRooster-RWに接続する事により㈱ウィルコムが提供する「WakeOnサービス」をRooster-RWで利用する事が可能となります。
待ち受け中のRooster-RWが㈱ウィルコムが提供するWakeOnセンター経由のWakeOnメッセージ、または㈱ウィルコムの端末からライトメールを受信すると、自動的に指定された外部ネットワークへダイヤルアップ接続します。また“アドレス解決機能”と併用することにより、使用用途が広がります。

● WakeOn VOICE 機能

WakeOn Voice機能は、音声着信可能なモバイルカードをRooster-RWに接続する事により、携帯電話機等からモバイルカードへの電話番号へ音声通話をトリガとし外部ネットワークへダイヤルアップ接続を開始します。
また、“アドレス解決機能”と併用することにより使用用途が広がります。

● FOMA LAN着信機能

FOMA端末モバイルカードをRooster-RWに接続することにより、㈱NTTドコモが法人向けサービス「FOMAによるLAN接続サービス」を利用する事が可能になります。Rooster-RWをクライアント側に設置する事で、FOMA網を利用したPUSH型の高セキュリティでリモートアクセス環境の構築が可能となります。

●リモートアクセス機能

Rooster-RWはPHS、FOMA対応カード端末による1回線収容のリモートアクセス機能を搭載しています。
社内LANなどのイントラネット環境に設置すれば、外部からモバイルカードなどによるダイヤルアップ接続環境を構築することが可能となります。
また不正アクセスを防ぐ高度なセキュリティとして、CLIDとPAP、CHAPの認証に対応しています。

●アドレス解決機能

Rooster-RWはプロバイダへ接続する度に変化するグローバルIPアドレスを、あらかじめ設定されているメールアドレスへ通知する事が可能です。
また、弊社と協業パートナー様が運営するダイナミックDNSサービスを使用することが可能です。
【「どこでもカメラ」ヴィ・インターネットオペレーションズ株式会社様　http://www.vio.co.jp】

● PPPoE 対応（フレッツ・ ADSL B フレッツ対応）

PPPoEに対応しておりますので、PPPoE認証が必要なプロバイダに接続する場合でも複数のパソコンから同時にインターネットアクセスが可能です。

● SPI（ステートフル・パケット・インスペクション）機能等、高性能ファイアウォール機能搭載

本格的なファイアウォール機能として、MACフィルタリング、IPフィルタリング、ポートフィルタリングの他にSPI機能を搭載しました。SPIではIPパケットのヘッダ情報のみではなくデータの内容やフラグの状態、特定のアプリケーションが複数のポートを使用して通信を行う場合に、1つのセッションとして認識してTCP、UDPののプロトコルまで含めて監視を行っている為、従来のパケットフィルタリングでは防ぐ事が出来なかった不正アクセスを防ぐことが可能です。

● WWW ブラウザによるウィザード形式簡単設定及びアップグレード可能

各種設定はパソコンのブラウザより本製品の設定ユーティリティにアクセスすることにより行えます。
また、ファームウェアのアップグレードも同様に可能です。

動作環境

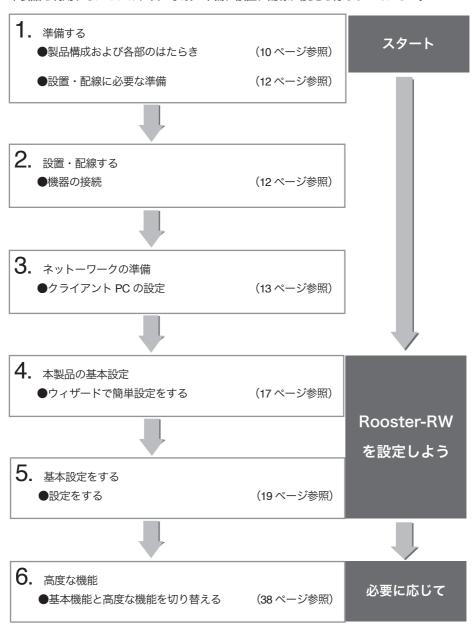
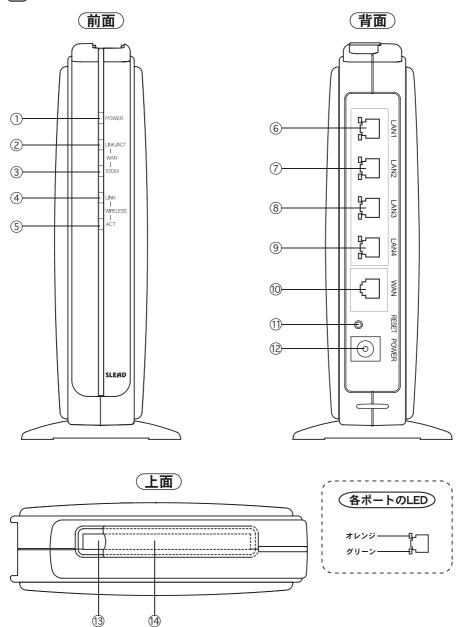
本製品は、WindowsOSに限らず、TCP/IPをサポートしているあらゆるOSに対応しています。
以下の環境でご使用ください。

- ●クライアント側は、Windows/95/98/Me/2000/XP/NT4.0/Vista、MacOS、UNIX、LinuxなどTCP/IPをサポートしているOSとなります。
- ●設定を行うためには、InternetExplorer6.0以降が動作するOSが必要となります。

ご使用までの流れ

本製品を利用するためには、次の手順で準備、設置、配線、設定を行なってください。

各部の名称とはたらき

前面
背面
①
POWER
②
LINK/ACT
WAN
③
100M
④
LINK
WIRELESS
⑤
ACT
SLEAD
⑥
LAN1
⑦
LAN2
⑧
LAN3
⑨
LAN4
⑩
WAN
⑪
RESET
⑫
POWER
上面
⑬
⑭
各ポートのLED
オレンジ
グリーン

1）POWER ランプ

本製品の電源が入っている場合は、グリーンの LED が点灯します。この LED が消灯している場合は、本製品の電源が入っていないことを表します。

2）LINK/ACT ランプ

WAN ポートにケーブルがつながれているときに点灯します。WAN ポートにデータが流れると点滅します。

3）100M ランプ

WAN ポートが 100BASE で接続されると点灯します。

4）LINK ランプ

モバイルカードの場合　－ リンクすると点灯します。（ダイヤル中は点滅します。）
RoosterCard 場合　－ リンクすると点灯します。

5）ACT ランプ

モバイルカードの場合　－ データが流れると点滅します。
RoosterCard 場合　－ データが流れると点滅します。

6）LAN ポート 1

LAN ポートです。ローカルネットワーク側の PC もしくは HUB を接続します。

7）LAN ポート 2

LAN ポートです。ローカルネットワーク側の PC もしくは HUB を接続します。

8）LAN ポート 3

LAN ポートです。ローカルネットワーク側の PC もしくは HUB を接続します。

9）LAN ポート 4

LAN ポートです。ローカルネットワーク側の PC もしくは HUB を接続します。

※ 6 ～ 9 の各ポートの LED について

グリーン LED － ケーブルがつながれているときに点灯し、データが流れると点滅します。
オレンジ LED － 100BASE で接続されると点灯します。

10）WAN

WAN ポートです。ブロードバンド ネットワーク プロバイダに接続する ADSL モデムやケーブルモデムを接続します。モバイルカードと同時に使用することはできません。

11）RESET スイッチ

本製品を再起動します。プラスティック製のピンなどを使って押してください。工場出荷時の設定に戻すには、6 秒以上押し続けてください。

12）POWER

付属している AC アダプタのコネクタを差し込むジャックです。

13）カード取り出しボタン

本製品からカードを取り出すときに押すボタンです

14）カード差し込み口

本製品へカードを差し込む口です。

ハードウェアの準備

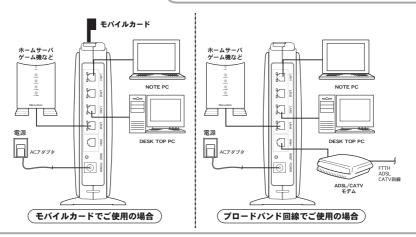
本製品と接続するために必要な環境と、本製品との接続方法を説明します。

必要な環境

- TCP/IP が利用できる OS(Windows 、 MacOS 、各種 UNIX など)を搭載し、Ethernet ポートを装備した PC
- UPT ケーブル
- ブロードバンド回線(ブロードバンドルータとして使用する場合)
- モバイルカード(AIR-EDGE 叉は FOMA 、b-mobile などの各種モバイルカードを使用する場合)
- Internet Explorer 6.0 以上

接続方法

1. 本製品と PCの電源が入っていないことを確認してください。
2. LAN ポートにクライアントとなる PC を接続して下さい。
3. モバイルカード を接続して下さい。
4. 本製品の電源コネクタに AC アダプタを接続して下さい。
   次に AC アダプタをコンセントに接続して下さい。
5. PC の電源を入れて下さい。

■カード挿入時の注意
Rooster のロゴマークのある面にカード本体の正面がくるようにして、カードを挿入してください。
CF タイプのカードの場合は、必ず CF カードアダプタを接続してください。

- モバイルカード、を使用する場合は、必ず電源を切った状態でカードの抜き差しを行ってください。電源を入れた状態でカードの抜き差しを行うと、本製品が作動いたしません。
- AC アダプタは、必ず付属のものを使用して下さい。付属以外の AC アダプタを使用すると、故障・誤作動の原因になります。付属以外の AC アダプタを使用した場合の故障は、保証対象外となります。
- カード取り出しボタンはまっすぐ押して下さい。

ネットワークの準備

この章では、本製品の設定をする前にすべきことを説明します。

ご利用環境の確認

1．ご利用の PC に LAN 環境は用意されていますか？
本製品と PC を接続する為には PC に LAN 環境が必要です。LAN 環境が無い場合には、ご利用の PC にあわせて LAN 機器をご用意ください。
●デスクトップ PC の場合
LAN ポートが標準で装備されていない場合、LAN ボードをご利用の PC にあわせて増設してください。
●ノート PC の場合
LAN ポートが標準で装備されていない場合、LAN カードをご利用の PC にあわせて増設してください。
2．モバイルカードまたは CATV/ADSL モデム、接続する LAN ケーブルは準備できていますか？
3．通信事業者との契約は完了していますか？
＜インターネット接続の場合＞
●電話線、光ケーブル、モバイルカード等の回線事業者との契約、工事が完了している必要があります。(NTT(株)、YahooBB、(株)NTT ドコモ、(株) ウィルコム、日本通信 (株)　等)
●インターネット接続サービスであるプロバイダ (ISP) への契約の完了している必要があります。
(OCN、NIFTY　等)（事業者によっては回線事業者とプロバイダが同じ契約の場合があります、その場合別途プロバイダへの契約は必要ありません)
●本製品の設定には、以下の情報が必要になります。
プロバイダとの契約時に提供されている情報をご用意ください。不明な場合はご契約のプロバイダへお問い合わせください。
・PPPoE 接続の場合（フレッツ等）
ユーザ名、パスワード。
サービス名、DNS サーバの IP アドレス。（プロバイダ指定の場合）
・DHCP をご利用の場合（YahooBB 等）
コンピュータ名、DNS サーバの IP アドレス。（プロバイダ指定の場合）
・固定 IP アドレスで接続の場合
WAN 側の IP アドレス、サブネットマスク、ゲートウェイ IP アドレス、DNS サーバの IP アドレス。
・モバイルカードをご利用の場合
アクセスポイントへの電話番号、ユーザ名、パスワード。
DNS サーバの IP アドレス。（プロバイダ指定の場合）
＜ RAS として使用する場合＞
モバイルカードの通信事業者（(株)NTT ドコモ、(株) ウィルコム、日本通信 (株)）との契約が完了している必要があります。

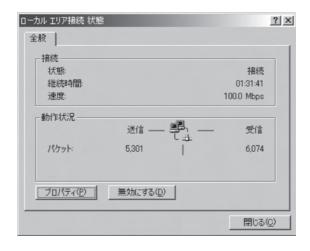
●回線事業者（プロバイダ）によってはルータを使ってのインターネットアクセスを禁止している場合があります。事前にご確認ください。
● LAN 型 PPPoE 接続（un numbered 接続）には対応しておりません。
●回線事業者（プロバイダ）によっては、ADSL/ ケーブルモデムに接続する機器の MAC アドレスの申請が必要な場合があります。その場合は本製品の MAC アドレスを確認してください。確認方法は 46 ページの MAC アドレスの変更を参照してください。

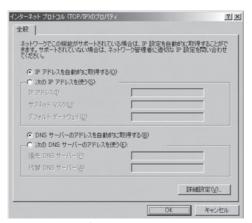
クライアント PC の設定

本製品にアクセスできるように、クライアント PC に DHCP クライアントの設定をします。
DHCP を使用しない場合は、各 PC に手動で IP を設定する必要があります。その方法については、ネットワークカード及び Windows のマニュアル等を参照してください。

手動で IP を設定する場合は DNS サーバのアドレスも手動で設定してください。

DHCP を使用する設定

1．スタートメニューをクリックし、「設定」→「ネットワークとダイアルアップの設定」→「ローカルエリア接続」をダブルクリックします。

2．プロパティをクリックします。

3．「インターネットプロトコル（TCP/IP)」をクリックし、「プロパティ」をクリックします。
TCP/IP プロパティダイアログが表示されます。

4．「IP アドレスを自動的に取得する」、「DNS サーバのアドレスを自動的に取得する」を
選択します。

5．OK をクリックし、PC を再起動してください。

この設定方法は Windows2000 のものです。
Windows95/98/ME、WindowsNT、WindowsXP をお使いの方は、47 ～ 48 ページを参照してください。

プロバイダ情報の確認（インターネット接続する場合）

ルータの設定をする前に、次のようなプロバイダ情報をご用意ください。

モバイルカードをお使いの場合

●プロバイダの電話番号
使用するコースによって電話番号が異なりますので、お間違えのないように十分ご注意ください。
●ユーザー名
●パスワード
●ネームサーバ（DNS サーバ）の IP アドレス（必要な場合）

モバイルカードを用いてデータ通信を行う場合には、モバイルカードと回線事業者との回線契約が必要です。

ブロードバンドルータとしてお使いの場合

プロバイダから固定 IP アドレスを受けている場合
● IP アドレス
●サブネットマスク
●ゲートウェイ
● DNS（ネームサーバ）

PPPoE を使用する場合
●ユーザー名
●パスワード

これらの情報がわからない場合は、プロバイダに確認してください。

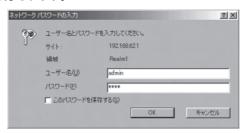
本製品の基本設定

基本的な管理上の機能には、設定、グローバルアドレス、モバイルカード、ツール、ステータス、DHCP、ログなどがあります。ウィザード設定を使用することにより、本製品に必要な最低限の情報を簡単に設定することができます。
本製品は、Web ベースの設定ツールを使用し、設定をカスタマイズすることができます。ネットワーク上のクライアント PC から、アクセスすることができます。

●設定ツールにアクセスするには、Microsoft Internet Explorer 6.0 か、それ以上のブラウザを使用してください。
●ブラウザでプロキシを使用する設定がされていると設定画面が表示されません。プロキシ設定を無効にしてください。ブラウザの設定変更方法については、49 ページを参照してください。

Web ベースの設定ツールを開く

1. ブラウザを開いてください。
2. URL 欄に「http://192.168.62.1」と入力して、Enter キーを押してください。

ログオンダイアログが表示されます。

3. ユーザーネームに「admin」と入力し、次にパスワードを入力して、OK をクリックしてください。デフォルトパスワードは「1234」です。
   本製品の設定ツールが表示されます。

Web ベースの設定ツールは、一定のアイドル時間があると、ログアウト処理されます。その場合は、もう一度ユーザー名とパスワードを入力してください。

ここで使用するユーザー名とパスワードは、本製品の設定ツールにアクセスするためのものです。プロバイダから提供されるものとは異なりますので、ご注意下さい。

ウィザードで簡単設定をする

本製品の設定ツールにアクセスすると、以下のような画面が表示されます。

使用される用途に応じて基本的な設定をウィザード形式で行ないます。
ウィザードでの設定は、あくまでも基本的な設定であり、設定後も設定の変更･修正、更に高度な設定を行なう事が出来ます。

ウィザードで表示される項目に必要事項を入力、あるいは選択肢を選んでください。入力した項目でよければ「次へ」、前の画面に戻る場合は「戻る」、設定を入力前に戻す場合は「キャンセル」をクリックしてください。
設定が終了すると、その旨表示されます。
ウィザードによる簡単設定を終えた後は、Rooster-RW は設定された動作を行ないます。引き続き画面左の「基本設定」、「高度な設定」でより細かな設定を行なう事も出来ます。

基本設定をする

設定

ホスト名、ドメイン名、LAN の IP アドレス、WAN の IP アドレス、PPPoE ログインなど、本製品の基本的な設定を行います。

設定 | アドレス解決 | 無線LAN | モバイルカード | ツール | ステータス | DHCP | ログ | 統計 | 高度な設定 | ヘルプ

ホスト名: (ISPによっては必須です)
ドメイン名: (ISPによっては必須です)
ファームウェア バージョン: 00.07.13(RW-H), Mar 24 2005
LAN IPアドレス:
IPアドレス: 192 . 168 . 62 . 1
サブネットマスク: 255 . 255 . 255 . 0
WAN/RAS IPアドレス:
IPアドレスを自動で取得する
IPアドレスを指定する
WAN IPアドレス / 本機側割り当てIPアドレス: 192 . 168 . 0 . 1
サブネットマスク: 255 . 255 . 255 . 0 (RAS動作時は未使用)
ゲートウェイ / クライアント割り当てIPアドレス: 192 . 168 . 0 . 2
DNSサーバ 1: 0 . 0 . 0 . 0
2: 0 . 0 . 0 . 0
PPPoE: 使用する 使用しない
ユーザー名:
パスワード:
WANハートビート: 使用する 使用しない
監視時間: 0 分
無応答時の動作: 無応答が連続して発生した場合、本機をリセットする
ログに記録する

設定 キャンセル ヘルプ

Roosterの基本的な設定をするためには、この画面で設定してください。
Air H"やP-inなどのモバイルカードを使用する場合は「モバイルカード」の画面で設定してください。

【注意】WAN/RAS IPアドレスの設定は、モバイルカードのダイヤルアップ時にも使用されます。(PPPoEを除く全てのWANアクセスで使用されます)

【注意】Air H",PPPoEや、pingに応答しないゲートウェイでは、WANハートビート機能は正常に動作しません。

- この取扱説明書の設定画面と実際の画面は、一部異なる部分があるかもしれません。ここで使われている画面写真は一例としてください。
- プロバイダから配布される PPPoE 接続ソフトウェアを PC にインストールする必要はありません。インストールしてある場合は、ソフトウェアを無効にしてください。

セットアップパラメータの設定

1. ホスト名を入力してください（オプション）。プロバイダによって、入力が必須になる場合があります。この情報がはっきりしない場合は、プロバイダに確認してください。
2. プロバイダのドメイン名を入力してください（オプション）。プロバイダによって、入力が必須になる場合があります。この情報がはっきりしない場合は、プロバイダに確認してください。
3. ファームウェアのバージョンを確認できます。
   この値は、現在使用しているファームウェアのバージョンおよび日付です。
4. 必要な場合は、IP アドレスを変更してください。通常は変更する必要はありません。

DHCP サーバ実行中に LAN の IP を変更するには、クライアント PC を再起動する必要があります。DHCP サーバを実行せずに LAN の IP アドレスを変更した場合は、ネットワーク内全てのクライアント PC の IP アドレスを手動で変更する必要があります。

5. WAN の IP アドレスについては、「IP アドレスを自動取得する」か、「IP アドレスを指定する」のどちらかを選択してください。IP アドレスを指定する場合は、WANIP アドレス、サブネットマスク、ゲートウェイと DNS を入力してください。これらの情報は ISP から提供されます。
   この設定は、WAN ポート（PPPoE を除く）、モバイルカードでのダイヤルアップ接続（インターネット接続）もしくは RAS 接続時に使用する IP アドレスを設定します。
6. PPPoE はフレッツ等を使用する時設定します。ユーザー名とパスワードを設定することにより、プロバイダがインターネットに接続することを可能にします。
   プロバイダが PPPoE を使用する場合は、「使用する」を選択し、7 に進んでください。そうでなければ「使用しない」を選択し、8 に進んでください。

PPPoE を使用する場合は、ネットワーク上にある全ての PC の PPPoE 接続を解除してください。PPPoE とモバイルカードは併用できません。

7. PPPoE を使用する場合は、PPPoE ユーザー名とパスワードを入力してください。
8. 必要な場合、WAN ハートビートを設定してください。この機能は WAN の接続状態を逐次チェックするために使用します。WAN ハートビート機能を使用する場合は「使用する」を選択してください。使用しない場合は「使用しない」を設定し、11 へ進んでください。
9. WAN ハートビートを使用する場合は、監視時間を入力してください。
   設定された時間毎に WAN ゲートウェイへの接続状態を PING にて確認します。

AIR-EDGE カード ,CDMA 1X WIN カードでは WAN ゲートウェイが PING に反応しないため、この機能は使用できません。また、ネットワークシステムによっては同様に使用できない場合があります。

10. WAN ハートビートで WAN への接続確認に失敗した場合の動作を設定してください。
    失敗が連続した時（10 回）に本機をリセットすることが出来ます。その場合「無応答が連続して発生した場合、本機をリセットする」を選択してください。ログのみを残す場合「ログに記録する」を選択してください。

11. 選択した設定で良ければ「設定」をクリックして完了します。また、「キャンセル」をクリックすることで、設定を中止することができます。

アドレス解決

外部ネットワークから Rooster に接続する場合 Rooster に割り当てられたグローバル IP アドレスを知っておく必要がありますが、通常のプロバイダ契約ではインターネットに接続する度にグローバル IP アドレスが任意に変化してしまいます。外部の相手から接続できるようこの問題を解決するには、この設定を行ないます。

1. アドレス解決機能を使用する場合「使用する」を選択してください。
   使用しない場合「使用しない」を選択し、7 に進んでください。

2. アドレス解決を行なうためのサービスを選択します。
   メール送信（POPbeforeSMTP)
      メールにてグローバル IP アドレスを通知する場合使用します。プロバイダの
      メールサーバ（もしくは使用するメールサーバ）が POPbeforeSMTP 対応の場合、これを選択します。
   メール送信（ユーザ認証 SMTP)
      メールにてグローバル IP アドレスを通知する場合使用します。プロバイダのメールサーバ（もしくは使用するメールサーバ）がユーザ認証 SMTP の場合、これを選択します。
   どこでもカメラ
      ヴィ・インターネットオペレーションズ株式会社　http://www.vio.co.jp
   DynDns.org
      Dynamic DNS Network Services
      http://www.dyndns.co.jp/
      DynDNS.org サービスはできる限り試用でのみお使いいただくことをお勧めします。長期間に及ぶ運用用途でご使用の場合は十分に動作検証を行って下さい。恐れ入りますが、弊社ではこの場合の動作保証及び責任につきましては一切負いかねます。ご了承願います。

SunComm.DDNS

http://www.sun-denshi.co.jp/sc
弊社が独自に実装したダイナミック DNS のプロトコルです。詳細につきましては弊社宛にご連絡願います。なお、弊社ではダイナミック DNS の運用は行っておりません。運用サーバー自体は、秘密保持契約成立後、弊社よりお渡しするプロトコル仕様一覧に基づいて、お客様側で設置をしていただくことになります。また、ご利用は法人のお客様に限らせていただきます。

3. 各種サービスの設定を行ないます。

●メール送信(POPbeforeSMTP)の場合

. 使用する SMTP サーバ名、POP3 サーバ名を入力してください。
. 使用する POP3 のアカウント名、パスワードを入力してください。
. 送信先メールアドレスに、グローバル IP アドレスを通知するメールアドレスを入力してください。
. 送信元メールアドレスに、送信するメールの送信者となるメールアドレスを入力してください。(入力しない場合、メールサーバによってはメールが送信されない場合があります)

●メール送信(ユーザ認証 SMTP)の場合

. 使用する SMTP サーバ名を入力してください。
. SMTP サーバのアカウント名、パスワードを入力してください。
. 送信先メールアドレスに、グローバル IP アドレスを通知するメールアドレスを入力してください。
. 送信元メールアドレスに、送信するメールの送信者となるメールアドレスを入力してください。(入力しない場合、メールサーバによってはメールが送信されない場合があります)

●どこでもカメラ、Dyn.Dns.org、SunComm DDNS の場合

契約したときに指定される DDNS サーバ名、アカウント名、パスワード、ホスト名を入力してください。

4. メール送信を指定した場合、メール送信のメッセージ内容を設定してください。
独自に指定する場合「指定のメッセージを送信する」を選択してください。標準のメッセージを使用する場合「標準のメッセージを送信する」を選択し、6 に進んでください。
標準のメッセージは、以下のような形式となります。

＜例＞

タイトル:　Rooster IP Report
送信者:　Rooster(004053010203) <from@mailaddress>
　　↑カッコ内は　Rooster-RW の MAC アドレス
内容:　Rooster IP-Address Report v0.00.

MAC=004053010203　　← Rooster-RW の MAC アドレス
IP=10.20.30.40　　←割り当てられているグローバル IP アドレス

5. メール送信で指定のメッセージを送信する場合、指定のメッセージを入力します。
この入力の文字列中の "%s" がグローバル IP アドレスに変換されます。
＜例＞

設定内容	実際に送信されるメッセージ （割り当てられているグローバル IP アドレスが 10.20.30.40 の場合）
http:// %s /mobile	→ http://10.20.30.40/mobile

注意
指定メッセージの最大設定入力文字数は60文字です。
送信されるIPアドレスも含みます。

6. 指定されたサービスを更新させるための更新時間を設定します。
この設定時間毎に指定されたサーバにアクセスを行ないます。
0を設定した場合、自動更新となりグローバル IP アドレスが変更された時のみサーバにアクセスします。
設定は最低5分ですので、5分以上を設定してください。

●メールでこの設定に0以外（自動更新以外）を設定した場合、設定された時間毎にメールを送ります。
●サービスのサーバの負荷低減のため、できるだけ0の自動更新をお使いください。

7. 選択した設定でよければ「設定」をクリックして完了します。また、「キャンセル」をクリックすることで設定を中止する事が出来ます。

無線 LAN

別売の RoosterCard を接続することで、11Mbps 無線 LAN アクセスポイントとして利用できます。無線 LAN アクセスポイントとしてご利用になる場合は、RoosterCard をご用意ください。無線 LAN を使用するには、無線 LAN の設定をしてください。無線 LAN を使用する／使用しない、ESSID、チャンネル、WEP（暗号化）という基本的な設定が必要です。

モバイルカードご使用の場合には、設定する必要はありません。モバイルカードと無線 LAN は同時にご使用になれません。

基本的な無線 LAN の設定

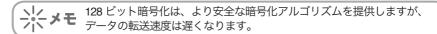
1. 最初に、無線 LAN でのアクセスを使用する／使用しないを選択してください。「使用する」を選択しない限り、無線 LAN の機能は使用できません。
2. ESSID（SSID と呼ばれることもあります）を入力してください。ESSID は、無線 LAN ネットワークの全てのクライアント PC に共有されている、ユニークな識別子です。32 文字を超えて登録することはできません。
3. チャンネル番号（1 から 11 まで）を入力してください。
4. WEP を使用する／使用しないを選択してください。「使用する」を選択した場合、セキュリティキーを設定するために、「WEP の設定」をクリックしてください。設定方法は、下記「WEP キーの設定」を参照して下さい。
5. 高度な無線 LAN の設定をしたい場合は、「高度な無線 LAN の設定」へ進んでください。
   無線 LAN の設定が終了したら、設定を有効にするために「設定」をクリックして完了します。
   また「キャンセル」をクリックすることで、設定を中止することができます。

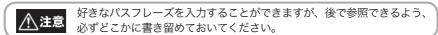
⚠注意 他社の無線 LAN カードでは、ご利用いただけません。必ず RoosterCard をご利用ください。

WEP キーの設定

1. セキュリティキーを入力するウィンドウを開くには、「WEP の設定」をクリックしてください。

2. 暗号化レベル（64 ビットか 128 ビット）を選択してください。

128 ビット暗号化は、より安全な暗号化アルゴリズムを提供しますが、データの転送速度は遅くなります。

3. パスフレーズを入力し「生成」をクリックするか、手動で 4 つまでのキーを入力することにより WEP キーを指定してください。「キーのクリア」をクリックすることにより、キー情報を削除することができます。

好きなパスフレーズを入力することができますが、後で参照できるよう、必ずどこかに書き留めておいてください。

4. デフォルト TX キーをドロップダウンリストから選択してください。
   この値は、使用されるデフォルトの暗号化キーを決定します。
5. 選択した設定で良ければ「設定」をクリックして完了します。
   また「キャンセル」をクリックすることで、設定を中止することができます。「再読込」をクリックすると、最新のデータが確認できます。
6. 設定し終わったら、ウィンドウを閉じてください。

高度な無線 LAN の設定

通常は高度な設定を行う必要はありません。変更が必要な場合以外は、デフォルト設定のままでご使用ください。

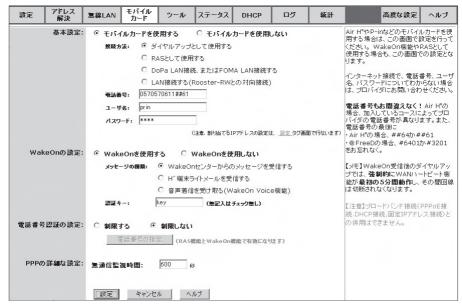
1．ファームウェアのバージョン
　現在使用している無線のファームウェアのバージョンを示しています。
2．ビーコン間隔
　これは、アクセスポイントによってブロードキャストされる間隔です。
　画面右のテーブルの中で、高度な無線の設定に対するデフォルトの値を表示していますので、参考にしてください。
3．RTS のしきい値
　データ/
4．フラグメ
　長いパケ
5．DTIM 間
　このパラ

別売の RoosterCard が生産完了のため
無線 LAN の機能はご利用いただけません。

6．最大ステーション数
　このパラメータは、関連付けされた無線 LAN のステーションの最大数を指定します。
7．基本レート
　「1-2-5.5-11MBps」か「1-2MBps」から選択してください。
8．TX レート
　「1-2-5.5-11MBps」か「1-2MBps」から選択してください。
9．ヘッダタイプ
　「72 ビット」か「144 ビット」から選択してください。
10．証明方法
　「オープンシステム」「共有キー」「すべて」から選択してください。
11．強化セキュリティ対策
　「使用する」を選択すると、ESSID を隠し、ESSID を指定していない PC からの接続を無効にすることができます。
12．選択した設定で良ければ「設定」をクリックして完了します。また「キャンセル」をクリックすることで、設定を中止することができます。

モバイルカード

モバイルカードでインターネットへ接続する場合、RAS 機能を使用する場合、FOMA LAN 接続する場合、WakeOn 機能を使用する場合に設定します。

ブロードバンドを使用する場合は、この機能を利用することは出来ません。

この取扱説明書の設定画面と実際の画面は、一部異なる部分があるかもしれません。ここで使われている画面写真は一例としてください。

基本設定

1. モバイルカードを使用する場合「モバイルカードを使用する」を選択します。
   使用しない場合は「モバイルカードを使用しない」を選択し、11に進んでください。
2. 接続方法を選択してください。
   - ●インターネットへ接続する場合や、ダイヤルアップを行う場合、
     “ダイヤルアップとして使用する”を選択してください。
   - ●RASとして使用する場合
     “RASとして使用する”を選択してください。
   - ●㈱NTTドコモのFOMA LAN接続でクライアントとして使用する場合
     “DoPa LAN接続、またはFOMA LAN接続する”を選択してくだい。
3. “ダイヤルアップとして使用する”（インターネット接続する）場合、“DoPa LAN接続する”場合は、プロバイダの電話番号を入力してください。
   （電話番号の設定について詳しくは、30ページをお読みください）
   “RASとして使用する”場合は、設定する必要はありません。

間違った電話番号や違ったパラメータを設定すると通信事業者より意図しない課金がされてしまう可能性がありますので、十分ご注意ください。

4. ユーザー名、パスワードを入力します。
 ●“ダイヤルアップとして使用する”(インターネット接続する)場合、“DoPa LAN接続、または FOMA LAN接続する”場合は、プロバイダより指定されたユーザ名、パスワードを入力してください。
 ●“RASとして使用する”場合は、アクセスがあったユーザのユーザ認証をする為のユーザ名、パスワードを任意で入力してください。
5. WakeOn機能を使用する場合「WakeOnを使用する」を選択してください。
 使用しない場合「WakeOnを使用しない」を選択して8へ進んでください。
6. WakeOn機能で受け入れるWakeOnメッセージの種類を選択してください。
 ●“WakeOnセンターからのメッセージを受信する”を選択してください。
 WakeOnセンターを利用するには、別途㈱ウィルコムと契約をする必要があります。
 ●㈱ウィルコムの端末からライトメールを受信する場合は、“H"端末ライトメールを受信する”を選択してください。
 ●音声着信を受け取るWakeOn Voiceを使用する場合は、“音声着信を受け取る”を選択してください。

WakeOn機能をご利用頂くには、モバイルカードがその機能に対応している必要があります。詳しくは対応機種モード一覧表
(本取扱説明書の30ページをご覧ください。)

7. メッセージに認証キーによる認証を設定する場合、認証キーを入力します。
 (“WakeOnセンターからメッセージを受信する”、“H"端末からメッセージを受信する”場合のみ)
 認証キーは、受信したメッセージの先頭文字から設定された認証キー文字数分だけ文字を比較し、一致した場合は成功となります。1文字でも違った場合は失敗となります。
 認証キーは、半角英数字のみです。
 ＜例＞

設定した認証キー	受信したメッセージ	結果
1234	5678	→×(全く一致していない為)
1234	1234	→○(全文字が一致している為)
12	1234	→○(認証キー 2 文字が一致している為)
12345	1234	→×(5文字目が一致しない為)

8. RASとして使用の場合、もしくはWakeOnを使用の場合で、電話番号認証(CLID)を行う場合「制限する」を選択できます。行わない場合は「制限しない」を選択し、10へ進みます。

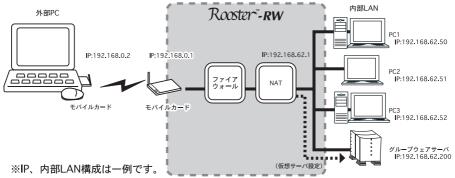
9. 「電話番号の指定」ボタンを押すことにより電話番号一覧表が表示されますので、ここにRAS接続、WakeOnメッセージ受信を許可する電話番号を入力します。

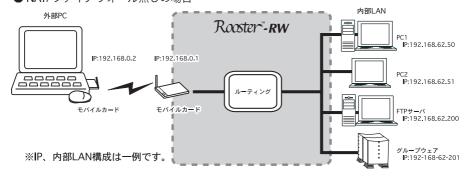
10. 無通信監視時間が、一定時間モバイルカードで通信が行われなかった時に自動的にモバイルカード接続を切断する時間を設定します。単位は秒です。(設定値は目安です)
 0を入力すると無通信時間を監視しませんので、自動的には切断しません。

０に設定しても、電波状態の影響による切断、プロバイダから切断された場合、本機からは積極的に再接続は行なわれません。再接続は LAN 側から接続要求、または本機の通信で接続の必要があった場合のみとなります。

11. 選択した設定でよければ、「設定」をクリックして完了します。また、「キャンセル」をクリックすることで設定を中止する事が出来ます。

RAS 機能でのネットワーク構成

● NAT/ ファイアウォール有りの場合（デフォルト）

外部 PC と内部 LAN の間には NAT/ ファイアウォールが入っており、外部 PC からは内部 LAN に自由にアクセスすることが出来ません。内部 LAN にアクセスする場合は、アクセスするマシンへ仮想サーバの設定、もしくは DMZ の設定が必要になります。（設定は 38 ページを参照）

● NAT/ ファイアウォール無しの場合

外部 PC と内部 LAN の間には通常のルーティングのみとなり、自由にアクセスすることが出来ます。外部からのアクセスセキュリティを考慮しない場合、自由度が高く、特に設定をしなくてもどのマシンへもアクセスが可能です

一般的には Rooster-RW の WAN 側 IP アドレスを固定にします。
19 ページ　WAN/RAS IP アドレス 参照

対応機種／対応通信モード一覧（2008年4月現在）

		ダイヤルアップ機能	リモートアクセス(RAS)	WakeOn	WakeOn Voice	FOMA LAN
㈱ウィルコム	CH-S203C/TD	○	○	○	−	−
	AX420S	○	○	○	○	−
	AX420N	○	○	○	−	−
	AX510N	○	○	○	−	−
	AX520N	○	○	○	−	−
	AX530IN	○	○	○	−	−
	TH-H301C	○ ※	−	−	−	−
㈱NTTドコモ	FOMA F2402	○	○	−	−	○
	FOMA P2402	○	○	−	−	○
	FOMA P2403	○	○	−	−	○
日本通信㈱	BMH11C-J	○	−	−	−	−
	BM-H1C2-150H	○	−	−	−	−
KDDI㈱	W01K	○	−	−	−	−
	W04K	○	−	−	−	−
	W05K	○	−	−	−	−
京セラコミュニケーションシステム㈱	S101C	○	−	−	−	−
ソフトバンクモバイル㈱	VC701SI	○	−	−	−	−
	C01SI	○	−	−	−	−

※㈱ウィルコムにお問い合わせください。

インターネット接続の料金コースと専用通信方式

通信業者	ご利用の料金コース	通信方式の名称	電話番号の形式
(株)ウィルコム	つなぎ放題、[8×]、[4×]	PRO8× 4x パケット方式	〈電話番号〉##64
	つなぎ放題、[1×]	1x パケット方式	〈電話番号〉##61
	ネット25、[8×]、[4×]	PRO8× 4x パケット方式	〈電話番号〉##64
	ネット25	フレックスチェンジ方式	〈電話番号〉##7
(株)NTTドコモ	FOMA	384kパケット通信	注1） *99* * *●#
		64k 回線交換	*9601
KDDI(株)	CDMA 1XWIN	3.6 Mパケット通信	*99* *24#
ソフトバンクモバイル(株)	アクセスインターネット	3.6 Mパケット通信	*99#
		64k 回線交換	*7300

※＜電話番号＞は各プロバイダでご利用の料金コースに応じたアクセス番号をご使用ください。
※●は、APN の設定で登録を行った cid 番号(1-10)が入ります。(mopera では初期値は "1" となります。)
　設定の詳細は、FOMA の取扱説明書等をご覧下さい。
※上記の通信速度は理論値です。ご使用の環境、時間帯によって通信速度が左右されますので、予めご了承ください。

＜ PIAFS 通信方式 ＞

通信業者	通信方式	電話番号の形式
(株)ウィルコム	PIAFS 32k	〈電話番号〉##3
	PIAFS 64k	〈電話番号〉##4

●ブロードバンド接続（PPPoE 接続、DHCP 接続、固定 IP アドレスとの接続）との併用はできません。
●パソコンに AIR-EDGE カードのドライバをインストールする必要はありません。
●モバイルカード付属のユーティリティソフトウェアは、本製品経由では作動致しません。
●モバイルカードを用いて、データ通信を行うためには回線事業者との回線契約が必要です。
●モバイルカードのサービスエリア外（圏外）ではご使用できません。
（モバイルカードの表示ランプをご確認ください。）
●モバイルカードのサービスエリア内でも電波の弱い場合は、通信が不安定になる恐れがあります。
●モバイルカードのサービスエリア内でも回線が混んでいて通信できない場合があります。
●データ圧縮機能はご利用になれません。

ツール

ツール画面では、以下の設定が行えます。

●本製品の管理者パスワードを変更
●設定を工場出荷時のものに戻す
●ファームウェアのアップグレード

初めて本製品にアクセスしたときは、パスワードを変更することを、強く推奨します。

設定 | アドレス解決 | 無線LAN | モバイルカード | ツール | ステータス | DHCP | ログ | 統計 | 高度な設定 | ヘルプ

パスワードの変更: 古いパスワード: 新しいパスワード: 再入力:
設定 キャンセル ヘルプ

工場出荷時の設定に戻す: ☐ デフォルトの設定に戻す。 実行 ヘルプ

ファームウェアのアップグレード: 参照... 実行 ヘルプ

メモ：アップグレードには約15秒かかります。その間、電源を切らないでください。

パスワードの変更、工場出荷時の設定に戻す、ファームウェアをアップグレードするには、この画面を使用してください。ルータに初めてアクセスした場合は、パスワードの変更を強く推奨します。

管理者パスワードの変更

1．古いパスワードを入力してください。工場出荷時のパスワードは「**1234**」です。
2．新しいパスワードを入力してください。パスワードは 64 文字まで入力できます。
3．確認のため、新しいパスワードを「再入力」にも入力してください。
4．「設定」をクリックすると変更され、「キャンセル」をクリックすると変更を元に戻せます。

メモ　セキュリティのため、パスワードは定期的に変更することを強く推奨します。

工場出荷時の設定に戻す

1．「デフォルトの設定に戻す」をクリックしてください。
　警告ダイアログが表示されます。
2．OK をクリックしてください。
　ルータの設定が工場出荷時の設定値にリストアされます。

メモ　ルータの設定を工場出荷時の設定に戻すには本体裏面にある RESET スイッチを押すことによっても可能です。（RESET スイッチを 6 秒以上押し続けてください。）

工場出荷時の設定に戻すと、ルータの全ての設定をリセットします。
一旦工場出荷時の設定に戻したら、初めからルータの設定を行う必要がありますので、デフォルト設定に戻す前に、今の設定をメモしておいてください。

ファームウェアのアップグレード

1. ファームウェアのイメージファイルを、本製品のウェブサイトからダウンロードし、PCのハードディスクに保存してください。
2. ファームウェアとパッチの場所をファームウェアのアップグレード欄に入力するか、「参照」をクリックして、ファイルを選択するダイアログボックスを表示してください。ダウンロードしたファームウェアの場所を選択し、「開く」をクリックしてください。
3. 「実行」をクリックしてください。ファームウェアがアップグレードされます。

ファームウェアのアップグレードには15秒ほどかかります。ファームウェアのアップグレード中は、本製品の電源を落とさないでください。

ステータス

ステータス画面は、本製品のステータスを確認できます。表示されるデータは、現在の設定によって変わります。

表示されるデータには、以下の情報があります。

- ●ホスト名
- ●ドメイン名
- ● PPPoE ログイン（使用する / 使用しない）
- ● LAN 設定（IP アドレス、サブネットマスク）
- ● WAN 設定（IP アドレス、サブネットマスク、ゲートウェイ、DNS）
- ● RAS 設定（IP アドレス、サブネットマスク、ゲートウェイ、DNS）

⚠注意

モバイルカードの通信を切断する場合は「切断」ボタンを押すことにより可能となりますが,再度インターネットに接続する場合は「接続」ボタンを押すまでモバイルカードは発信しません｡「切断」ボタンにより回線の切断を行った後、再度通信を行う場合には「接続」ボタンを押して下さい。

⚠注意

定額制モバイルカード以外のカードでご利用の場合はご注意下さい。TwoLinkDATAなどの通信時間により課金される回線交換方式のモバイルカードをご利用の場合は、通信終了時に必ず本製品の設定ユーティリティより“ステータス”のタブを選択し、モバイルカードの「切断」ボタンを押してください。再度通信を行う場合には「接続」ボタンを押してください。

DHCP の開放と再取得

設定画面で「IPアドレスを自動で取得する」と「PPPoEを使用しない」を選んだ場合、ステータス情報に「DHCP開放」と「DHCP再取得」ボタンが表示されます。これらのボタンを使うと、WANのIPアドレスを開放、再取得することができます。

WANのIPアドレス開放
- DHCP 開放をクリックする

WANのIPアドレス再取得
- DHCP 再取得をクリックする

DHCP

DHCP 画面では、DHCP サーバの設定をします。

メモ　本製品の DHCP の設定を無効にした場合、ネットワーク上の各PC の IP アドレスを手動で設定する必要があります。

DHCP サーバの設定

1．ネットワーク内に、すでに DHCP サーバが動いていないことを確認してください。
　また、各クライアント PC が、IP アドレスを自動で取得する設定になっていることを確認してください。
2．DHCP サーバ「使用する」をクリックしてください。
3．割り当てる最初の IP を入力してください。ここで指定する IP は、ネットワーク上の PC に割り当てる、最初の IP アドレスになります。
4．割り当てる最後 IP を入力してください。ここで指定するアドレスは、割り当てることのできる最後の IP アドレスになります。

例
開始アドレスを 192.168.1.51、終了アドレスを 192.168.1.100 にした場合、DHCP サーバはネットワーククライアントに 192.168.1.51 から 192.168.1.100 までのアドレスを与えます。

5．選択した設定で良ければ「設定」をクリックして完了します。また「キャンセル」をクリックすることで、設定を中止することができます。

DHCP テーブルの表示

「DHCP テーブルの表示」をクリックすると、DHCP サーバによって IP アドレスを割り当てられ、現在アクティブなクライアント PC の情報を表示します。

●インデックス番号
●クライアントのホスト名
●クライアントの IP アドレス
●クライアントの MAC アドレス

DHCP サーバの IP アドレスが、テーブルの一番上に表示されます。

「再読込」をクリックすると、表示されている情報を更新します。テーブルを見終わったら、ウィンドウを閉じてください。

アクティブなIPの一覧

再読込

DHCPサーバのIPアドレス:　192.168.9.10

Index	クライアントホスト名	IPアドレス	MACアドレス
	None	None	None

ログ

LAN と WAN のクライアントのアクセス履歴を記録するログファイルを確認できます。

パケットログ

(1) 通信ログ

通信ログをクリックすると、通信ログウィンドウが表示されます。テーブルには、インデックス番号、記録時間、通信タイプ、発信元 IP アドレス、発信元ポート、送信先 IP アドレス、送信先ポート、各イベントの終了した理由を表示します。
最新のデータを見るためには、再読込をクリックしてください。ログを見終わったら、ウィンドウを閉じてください。

通信ログ一覧

再読込

現在の時間は 0days 00:11:55

No.	記録時間	通信タイプ	発信元IP	発信元ポート	送信先IP	送信先ポート	終了した理由
1	0days 00:07:30	TCP	192.168.62.50	1028	202.239.172.79	80	NORMAL
2	0days 00:08:09	UDP	192.168.62.50	1026	61.198.138.14	53	TIMEOUT
3	0days 00:08:19	UDP	192.168.62.50	1027	61.198.138.14	53	TIMEOUT
4	0days 00:08:29	UDP	192.168.62.50	1029	61.198.138.14	53	TIMEOUT
5	0days 00:11:32	TCP	192.168.62.50	1033	202.239.162.254	80	NORMAL
6	0days 00:11:38	TCP	192.168.62.50	1032	202.239.162.254	80	NORMAL

閉じる

(2) 遮断ログ

遮断ログをクリックすると、遮断ログが表示されます。テーブルには、記録時間、インデックス番号、通信タイプ、発信元 IP アドレス、発信元ポート、送信先 IP アドレス、送信先ポート、各イベントの終了した理由を表示します。
最新のデータを見るためには、再読込をクリックしてください。ログを見終わったら、ウィンドウを閉じてください。
終了した理由の詳細は資料 1 （51 ページ）をご覧下さい。

遮断ログ一覧

再読込

現在の時間は 0days 00:13:34

No.	記録時間	通信タイプ	発信元IP	発信元ポート	送信先IP	送信先ポート	終了した理由
1	0days 00:06:00	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense
2	0days 00:11:21	TCP	61.240.246.46	44381	211.18.236.48	3389	Default Defense
3	0days 00:11:21	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense
4	0days 00:11:57	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense
5	0days 00:12:01	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense
6	0days 00:12:15	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense
7	0days 00:12:17	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense
8	0days 00:12:20	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense

閉じる

(3) 侵入ログ

侵入ログをクリックすると、侵入ログが表示されます。テーブルには、インデックス番号、記録時間、侵入タイプを表示します。
最新のデータを見るためには、再読込をクリックしてください。ログを見終わったら、ウィンドウを閉じてください。
侵入タイプの詳細は資料２（52 ページ）をご覧下さい。

侵入ログ一覧

再読込

現在の時間は 0days 00:14:24

No.	記録時間	侵入タイプ
1	0days 00:08:29	AscendKill

閉じる

(4) 無線通信ログ

侵入ログをクリックすると、侵入ログが表示されます。テーブルには、インデックス番号、記録時間、侵入タイプを表示します。

別売の RoosterCard が生産完了のため
無線 LAN の機能はご利用いただけません。

閉じる

モバイルログ

モバイルカード項目の ” 通信ログ ” をクリックすると、モバイルカードとの通信情報が表示されます。インデックス番号、記録時間、イベントの内容を表示します。

アドレス解決ログ

アドレス解決項目の ” 通信ログ ” をクリックすると、アドレス解決機能での通信ログが表示されます。インデックス番号、記録時間、イベントの内容を表示します。

WAN ハートビートログ

WAN ハートビート項目の ” 通信ログ ” をクリックすると、WAN ハートビート機能での通信結果等のログが表示されます。インデックス番号、記録時間、イベントの内容を表示します。

ログで表示される記録時間はログが記録された時間ですので、その事象が発生した時間と一致しない場合があります。

統計

LAN、WAN の通信状態を確認できます。

設定	アドレス解決	無線LAN	モバイルカード	ツール	ステータス	DHCP	ログ	統計	高度な設定	ヘルプ

再読込

この画面は、LAN、WAN、無線LANの通信状態を表示します。

LAN

Status: up Max.Mb/s: 100.0 IP Addr: 192.168.62.1 MAC Addr: 00:40:53:06:17:9c

受信		送信	
total bytes	185656	total bytes	637861
unicast pkts	226	unicast pkts	134
multicast pkts	1122	multicast pkts	1515
discards	0	discards	0
errors	0	errors	0
unknown protocols	13	packets queued	0

Mobile Card

Status: up Max.bps: --- IP Addr: 211.18.236.176 MAC Addr: ---

受信		送信	
total bytes	38282	total bytes	4926
unicast pkts	41	unicast pkts	53
multicast pkts	0	multicast pkts	0
discards	0	discards	0
errors	0	errors	0
unknown protocols	0	packets queued	0

無線LAN

Status: down Max.Mb/s: 11.0 IP Addr: 192.168.62.1 MAC Addr: 00:40:53:06:17:9c
SSID: WLAN

受信		送信	
unicast packets	0	unicast packets	0
multicast packets	0	multicast packets	0
fragments	0	fragments	0
unicast bytes	0	unicast bytes	0
multicast bytes	0	multicast bytes	0
fcs errors	0	deferred trans	0
discards no buffer	0	single retry packets	0
discards wepundecr	0	multiple retry packets	0
msg in msg frag	0	retry limit exceeded	0
msg in bad msg frag	0	discards	0
		discards wrong sa	0

LAN
LAN の現在のステータス、最大転送速度、IP アドレス、MAC アドレスの通信状態を表示します。

WAN 又はモバイルカード
WAN 又はモバイルカードの現在のステータス、最大転送速度、IP アドレス、MAC アドレスの通信状態を表示します。

最新のデータを見るためには、再読込をクリックしてください。ログを見終わったら、ウィンドウを閉じてください。

高度な機能

高度な管理者設定には､仮想（バーチャル）サーバ､フィルタリング､特別なアプリケーション､DMZ､MAC アドレスの変更が含まれます。

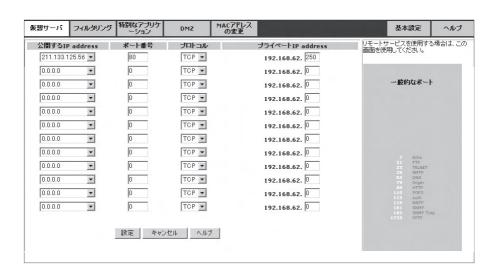
通常はこの機能を使用する必要はありません。

基本機能と高度な機能を切り替える

1. 基本機能の画面から、高度な機能の画面に切り替えるには、メニューバーの右端にある「高度な機能」をクリックします。
2. 一度高度な機能の設定の画面になったら、メニューバーの右端にある基本設定をクリックすることで基本機能に戻れます。

仮想（バーチャル）サーバ

外部ネットワークから FTP や Web 等のサーバを公開するためには、バーチャルサーバの設定が必要となります。

メモ　仮想（バーチャル）サーバを設定すると、フィルタリング画面でフィルタが自動的に設定されます。

仮想（バーチャル）サーバとしてネットワーク上の PC を設定

1．公開する IP アドレスのドロップダウンリストから、IP アドレスを選択してください。
WAN の IP アドレスで " 自動割り当て " を選択している場合、"AUTO" を選択して下さい。

DMZ 設定との併用はできません。

2．ポート番号を指定してください。どのポートを選ぶべきかについては、画面右の一般的なポートを参照してください。
3．ドロップダウンリストから、プロトコル（TCP、UDP、すべて）を選択してください。
4．プライベート IP アドレスを指定してください。アドレスの最後の部分のみ入力してください。
5．選択した設定で良ければ「設定」をクリックして完了します。「キャンセル」をクリックすることで、設定を中止することができます。。

仮想（バーチャル）サーバの削除

仮想（バーチャル）サーバを削除するには、公開する IP アドレス欄で「0.0.0.0」を選択し、「設定」をクリックしてください。

フィルタリング

ネットワークから通信するためのフィルタを設定します。本製品には、あらかじめいくつかのフィルタが設定されています。

⚠警告
●工場出荷時のフィルタ設定を上書きすると、ネットワーク内のクライアント PC がインターネットにアクセスできなくなる可能性があります。
●新しいフィルタを定義する場合は、設定されていない列に追加することをお勧めします。

フィルタの設定

1. フィルタリングのページのドロップダウンリストから、表示するページ（1 ～ 12、13 ～ 24、25 ～ 36）を選択してください。

36 個までのフィルタを定義できます。

2. ドロップダウンリストから、IP かポートフィルタリングを選択してください。
3. IP を選んだ場合、プロト番号（IP プロトコル番号、0 ～ 255）を入力してください。
   ポートフィルタリングを選んだ場合、4 に進んでください。

6（TCP）または 17（UDP）のプロト番号を入力すると、ポートフィルタリングが正しく動作しなくなります。

4. 方向のドロップダウンリストから、IN、OUT、すべてのいずれかを選択してください。
5. 2 でポートフィルタリングを選択した場合は、ポート番号（許可したいポート番号）を入力し、プロトコルのドロップダウンリストから TCP,UDP またはすべてを選択してください。2 で IP を選択した場合は、6 に進んでください。
6. MAC フィルタを設定するか、過去のフィルタリングオプションを設定したい場合は「MAC フィルタの設定」へ進んでください。

   フィルタリングの設定が終了し、設定を有効に変更したい場合は「設定」をクリック後再起動して下さい。、設定を元に戻す場合は「キャンセル」をクリックしてください。

警告
工場出荷時の設定に加え、いくつかのフィルタはバーチャルサーバ、特別なアプリケーションを使用可能にする為に自動生成される場合があります。

デフォルト設定

ID	フィルタリング種類	プロト番号	方向	ポート範囲	プロトコル	種類
1	ポート番号	0	OUT	80-80	TCP	HTTP､インターネットアクセス
2	ポート番号	0	OUT	53-53	UDP	DNS
3	ポート番号	0	OUT	25-25	TCP	SMTP
4	ポート番号	0	OUT	110-110	TCP	POP3
5	ポート番号	0	OUT	1720-1720	TCP	NetMeeting
6	ポート番号	0	OUT	1503-1503	TCP	NetMeeting
7	ポート番号	0	OUT	443-443	TCP	SSL
8	IP	1	IN/OUT	0	0	ICMP
9	ポート番号	0	OUT	21-21	TCP	FTP
10	ポート番号	0	IN	8001-8009	UDP	Rooster-RW 内部で使用

プライベート MAC フィルタリング

MAC アドレスから、特定の PC がインターネットにアクセスすることを拒否できます。

MAC フィルタの設定

1. MAC アクセスコントロールの画面を使用するため、「MAC フィルタの設定」ボタンをクリックしてください。

フィルタするMACアドレス

mac 1	00112233445
mac 2	00000000000
mac 3	00000000000
mac 4	00000000000
mac 5	00000000000
mac 6	00000000000
mac 7	00000000000
mac 8	00000000000
mac 9	00000000000
mac 10	00000000000

上記の図は、MAC アドレス 10 個分のみ表示しています。

2. ブロックしたい MAC アドレスを、テーブルへ入力してください。
   80 アドレスまでブロックできます。
3. テーブルの下にある「設定」をクリックし、ウィンドウを閉じてください。
4. フィルタオプションを追加する場合は、「フィルタオプションの追加設定」へ進んでください。
   フィルタの設定が終了し、設定を変更したい場合は「設定」をクリックして完了します。
   また「キャンセル」をクリックすることで、設定を中止することができます。

フィルタオプションの追加

リモート設定、IPSec パススルー、侵入検知といったフィルタオプションを使用することができます。

メモ　これらのオプションを変更すべきかどうかわからない場合は、デフォルト設定で使用することをお勧めします。

フィルタオプションの追加設定

1．それぞれのフィルタオプションで「使用する」か「使用しない」を選択してください。
　オプションには、以下の項目があります。
　【NAT】
　この項目を有効にすると、NAT の設定が可能になります。
　【ファイアウォール】
　この項目を有効にすると、ファイアウォールを使用し、ネットワークを保護することが可能になります。
　【リモート操作】
　この項目を有効にすると、WAN 側からポート番号 8080 を通じて本製品の設定ツールにアクセスできるようになります。
　【IPSec パススルー】
　この項目を有効にすると、IPSec パススルーを使用します。
　【PPTP パススルー】
　この項目を有効にすると、VPN を可能にするために PPTP を使用します。
　【侵入検知】
　この項目を有効にすると、外部からの攻撃を記録することができます。
2．選択した設定でよければ「設定」をクリックして完了します。「キャンセル」をクリックすることで設定を中止することができます。

フィルタの削除

フィルタリストから、既存のフィルタを削除することができます。

工場出荷時のデフォルトのフィルタ、バーチャルサーバや特別なアプリケーションに関係するフィルタを削除すると、サービスが使えなくなる可能性があります。

IP フィルタの削除

1．プロト番号欄に０を入力してください。
2．「設定」をクリックしてください。

ポートフィルタリングフィルタの削除

1．ポート番号欄に０を入力してください。
2．「設定」をクリックしてください。

特別なアプリケーション

この機能は、オンラインゲームやビデオ会議のようなマルチセッションアプリケーションに必要な場合があります。

メモ
特別なアプリケーションの設定を行うと、フィルタが自動作成される場合があります。

仮想サーバ | フィルタリング | 特別なアプリケーション | DMZ | MACアドレスの変更 | 基本設定 | ヘルプ

No.	プロトコル	ポート範囲	最大無通信時間	セッションチェーン	UDPチェーン	アドレス交換	アドレス変換	マルチホスト
1	TCP	21 - 21	3000	Disable	Enable	Disable	TCP	Enable
2	TCP	1720 - 1720	30000	Enable	Disable	Enable	TCP	Disable
3	TCP	1024 - 65535	30000	Enable	Enable	Enable	TCP	Enable
4	UDP	50000 - 65535	30000	Enable	Enable	Enable	TCP	Enable
5	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
6	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
7	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
8	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
9	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
10	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
11	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
12	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable

特定のポートを使用し、ネットワークの外側のPCと通信することを可能にするために、この画面を使用してください。この機能は、オンラインゲームやビデオ会議などに必要となる場合があります。

設定 キャンセル ヘルプ

一般的なアプリケーション: -- 選択してください -- Copy to No.: --

テーブルの最初の行は、FTP のためにあらかじめ作成されています。
これらを上書きすると、2 つの機能が使えなくなります。
FTP はパッシングモードをご利用下さい。

セッションチェーンは特定のアプリケーションソフトウェアが複数のポートを使用して通信を行う場合に、それらを 1 つのセッションとして認識して、高度なパケットフィルタを実現します。TCP だけでなく UDP パケットもセッション単位で監視します。

一般的なアプリケーションを設定する

1. 一般的なアプリケーションのドロップダウンリストから、適用したいアプリケーションを選択してください。
2. No. のドロップダウンリストから番号を選ぶことで、テーブルの特定のラインを選択してください。
3. Copy to をクリックしてください。設定されたアプリケーションがテーブルに表示されます。
4. 「設定」をクリックすると設定を変更し、「キャンセル」をクリックすると設定を元に戻します。

手動設定

手動で特別なアプリケーションの設定を行うことができますが、エキスパートなユーザーが行うべきです。どの設定をするべきかわからない場合は、一般的なアプリケーションの設定を使用することをお勧めします。

手動で特別なアプリケーションを設定

1. 設定する行を選んでください。

別のアプリケーションを登録するために現在の設定を上書きすると、上書きされたアプリケーションは使えなくなります。

2. ドロップダウンリストから、使用するプロトコル（TCP、UDP）を選択してください。
3. ポート範囲を指定してください。
   このパラメータは、アプリケーションが使用するポート番号を識別します。
4. 最大通信間隔を入力してください。
   このパラメータは、動的なセッションの最大間隔をミリ秒単位で入力します。
5. セッションチェーンのドロップダウンリストから、「使用する」か「使用しない」を選択してください。
6. 5 で「使用する」を選択していたら、UDP チェーンの「使用する」か「使用しない」かを選択できます。5 で「使用しない」を選んだ場合は、7 へ進んでください。
7. アドレス交換のドロップダウンリストから、「使用する」か「使用しない」を選択してください。このパラメータは、2 進法のアドレス置換を行うかどうかを設定します。
8. 7 で「使用する」を選択した場合は、アドレス変換から TCP か UDP を選択することができます。7 で「使用しない」を選択した場合は、9 へ進んでください。
9. マルチホストのドロップダウンリストから、「使用する」か「使用しない」を選択してください。このパラメータを有効にすると、異なる遠隔のホストから新しいセッションを開始することを可能にします。
10. 選択した設定で良ければ「設定」をクリックして完了します。また「キャンセル」をクリックすることで、設定を中止することができます。

特別なアプリケーションの削除

1. ポート範囲に「0-0」を入力してください。
2. 「設定」をクリックしてください。

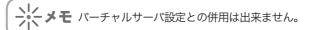
DMZ（LAN ポートを仮想 DMZ ポート化する場合）

ネットワーク上の 1 台以上の PC を公開するためには、DMZ 機能を使用します。この機能は、無制限の 2 ウェイコミュニケーションを要求する、オンラインゲームやホームサーバなどに使用します。

DMZ として指定する PC に対して、ファイアウォールは働きません。
セキュリティには十分ご注意ください。

DMZ ホストしての設定

1．公開される IP アドレスを、ドロップダウンリストから選択してください。
WAN の IP アドレスで “ 自動割り当て ” を選択している場合、“AUTO” を選択して下さい。

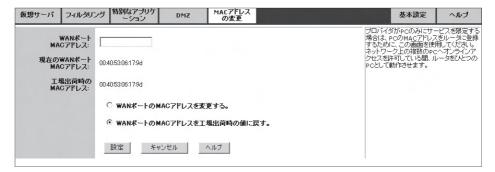
バーチャルサーバ設定との併用は出来ません。

2．プライベート IP アドレスを指定します。アドレスの最後の部分を入力してください。
3．選択した設定で良ければ「設定」をクリックして完了します。また「キャンセル」をクリックすることで、設定を中止することができます。

DMZ ホストの削除

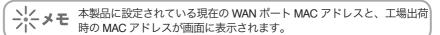
DMZ ホストを削除するには、公開する IP アドレスで「0.0.0.0」を選択し、「設定」をクリックしてください。

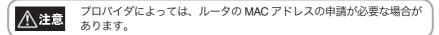
MAC アドレスの変更

本製品の WAN ポートの MAC アドレスを変更します。通常、変更する必要はありません。プロバイダにすでに PC の MAC アドレスを登録している場合、本製品の MAC アドレスを登録済みの MAC アドレスに変更することにより、プロバイダへの登録変更をしなくてもご利用いただけます。

モバイルカードでご使用の場合には、変更する必要はありません。

MAC アドレスの変更

1. プロバイダに登録した LAN カードの MAC アドレスを使用する必要がある場合があります。

メモ　本製品に設定されている現在の WAN ポート MAC アドレスと、工場出荷時の MAC アドレスが画面に表示されます。

2. 「MAC アドレス変更」をクリックすると設定を変更し、「MAC アドレス復旧」をクリックすると設定を工場出荷時に戻します。

注意　プロバイダによっては、ルータの MAC アドレスの申請が必要な場合があります。

補足説明：クライアント PC の設定　95/98/Me/2000/XP

本製品を利用してインターネット接続が出来るように、ご利用になる PC のネットワーク設定を行うことが必要です。ご利用になる PC のネットワークアダプタ設定、TCP/IP 設定を確認してください。（ご利用になる PC、OS 等によって確認方法は異なります）

複数の PC でインターネット接続を行う場合、全ての PC でネットワーク設定が必要です。

Windows XP で利用の場合の設定方法

※ご利用になる PC に LAN 環境が用意されていることを確認してください。

1) コンピュータ管理者または同等の権限のユーザー名でログオンしてください。
2) コントロールパネルをクリックしてください。
3) コントロールパネルにあるネットワークとインターネット接続をクリックしてください。
　※ネットワークとインターネット接続が表示されてなく、コントロールパネル内に幾つかのアイコン表示がされている場合は、そのまま４へお進みください。
4) ネットワーク接続をクリックしてください。
5) ローカルエリア接続を右クリックして、プロパティを選択してください。
6) 全般のタブ内のインターネットプロトコル（TCP/IP）がチェック（有効）されていることを確認してください。
　※機種によっては全般のタブ内に表示されていない場合があります。
　その場合は表示されている内容をご確認下さい。ローカルエリア接続の他にネットワークブリッジなどが存在している場合がありますので、表示されている内容に従い本操作をやり直してください。
7) インターネットプロトコル（TCP/IP）を選択してプロパティをクリックしてください。
8) 全般のタブ内にある IP アドレスを自動的に取得すると DNS サーバーのアドレスを自動的に取得するを選択し詳細設定をクリックしてください。
9)OK ボタンをクリックして設定を完了してください。（各プロパティ画面の OK ボタンをクリックします）
10)PC を再起動してください。
11)Web ブラウザで本製品を設定してください。

＜プロバイダからドメイン名の指定がされている場合のみお進みください＞
12)TCP/IP 詳細設定画面の DNS タブをクリックしてださい。
13)DNS タブ内にある以下の DNS サフィックスを順に追加するを選択してください。
14) 追加ボタンをクリックしてください。
15) プロバイダから指定されたドメイン名を入力してください。
16)OK ボタンをクリックして設定を完了してください。

Windows 95/98/Me でご利用の場合の設定方法

※ご利用になる PC に LAN 環境が用意されていることを確認してください。

1) コントロールパネルをクリックしてください。
2) ネットワークのアイコンをダブルクリックしてください。
3) ネットワークの設定タブ内の現在のネットワークコンポーネントの一覧表内にある TCP/IP →××××（ご利用中の PC に採用されている LAN 機器名が表示されます。機器により名称が異なります）を選択してプロパティのボタンをクリックしてください。
4)IP アドレスタブ内で IP アドレスを自動的に取得を選択してください。
5)OK ボタンをクリックして設定を完了してください。（各プロパティ画面の OK ボタンをクリックします）
6)PC を再起動してください。
7)Web ブラウザで本製品を設定してください。

<プロバイダからドメイン名の指定がされている場合のみお進みください>

8)TCP/IP プロパティ画面の DNS 設定タブをクリックしてださい。
9)DNS 設定タブ内にあるドメインサフィックスの検索順の設定スペース内にプロバイダから指定されたドメイン名を入力してください。
10) 追加ボタンをクリックしてください。
11)OK ボタンをクリックして設定を完了してください。

Windows の OS 用ディスクを入れるようダイアログが表示された場合は、メッセージに従って操作してください。

< TCP/IP がインストールされていない場合のみお進みください>

10) コントロールパネルをクリックしてください。
11) ネットワークのアイコンをダブルクリックしてください。
12) ネットワーク画面内の追加ボタンをクリックしてください。
13) ネットワークコンポーネントの種類の選択画面でプロトコルを選択して追加ボタンをクリックしてください。
14) ネットワークプロトコルの選択画面内の製造元で Microsoft を選択してください。
15) ネットワークプロトコルの選択画面内のネットワークプロトコルでTCP/IP を選択してください。
16)OK ボタンをクリックしてください。
17) 現在のネットワークコンポーネント一覧内に TCP/IP →××××（ご利用中の PC に採用されている LAN 機器名が表示されます。機器により名称が異なります）が追加されていることを確認してください。
18)OK ボタンをクリックして設定を完了してください。
19)PC を再起動させてください。

Windows 2000 でご利用の場合の設定方法

※ご利用になる PC に LAN 環境が用意されていることを確認してください。

1) コンピュータ管理者または同等の権限のユーザー名でログオンしてください。
2) スタートメニューから設定をクリックしてください。
3) ネットワークとダイアルアップ接続をクリックしてください。
4) ローカルエリア接続を右クリックして、プロパティを選択してください。
5) 全般のタブ内のインターネットプロトコル（TCP/IP）がチェック（有効）されていることを確認してください。
6) インターネットプロトコル（TCP/IP）を選択してプロパティをクリックしてください。
7) 全般のタブ内にある「IP アドレスを自動的に取得する」と「DNS サーバーのアドレスを自動的に取得する」を選択してください。
8)DNS サーバのアドレスを自動的に取得するのチェックをしてください。
9)OK ボタンをクリックして設定を完了してください。(各プロパティ画面の OK ボタンをクリックします)
10)PC を再起動してください。
11)Web ブラウザで本製品を設定してください。

<プロバイダからドメイン名の指定がされている場合のみお進みください>
12)TCP/IP 詳細設定画面の DNS タブをクリックしてださい。
13)DNS タブ内にある以下の DNS サフィックスを順に追加するを選択してください。
14) 追加ボタンをクリックしてください。
15) プロバイダから指定されたドメイン名を入力してください。
16)OK ボタンをクリックして設定を完了してください。

< TCP/IP がインストールされていない場合のみお進みください>
17) スタートメニューから設定をクリックしてください。
18) ネットワークとダイアルアップ接続をクリックしてください。
19) ローカルエリア接続を右クリックして、プロパティを選択してください。
20) ローカルエリア接続画面でインストールボタンをクリックしてください。
21) ネットワークコンポーネントの種類の選択画面でプロトコルを選択して追加ボタンをクリックしてください。
22) ネットワークプロトコルの選択画面内のネットワークプロトコルで TCP/IP を選択してください。
23)OK ボタンをクリックしてください

Web ブラウザの設定

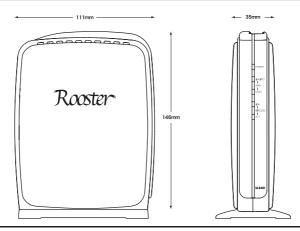
本製品は Web ブラウザを使用して設定を変更することができます。本製品の設定を行うために、Web ブラウザに下記のような設定をしてください。(InternetExplorer 6.0 の場合)

1)InternetExplorer を起動してください。
2) ツールからインターネットオプションをクリックしてください。
3) インターネットオプション画面の接続タブをクリックしてください。
4)LAN 設定ボタンをクリックしてください。
5) ローカルエリアネットワーク（LAN）設定画面内の「設定を自動的に検出する」のチェックをはずしてください。
6) ローカルエリアネットワーク（LAN）設定画面内の「自動構成スクリプトを使用する」のチェックをはずしてください。
7) ローカルエリアネットワーク（LAN）設定画面内の「LAN にプロキシサーバを使用する」のチェックをはずしてください。
8)OK ボタンをクリックして設定を完了してください。

仕様

ハードウェア仕様

製品名	Rooster-RW(SC-RS5FJ)	
ルーティング方式	スタティックルーティング	
サポート規格	LAN 側	IEEE802.3(10BASE-T Ethernet)
		IEEE802.3u(100BASE-TX Fast Ethernet)
	WAN 側	IEEE802.3(10BASE-T Ethernet)
		IEEE802.3u(100BASE-TX Fast Ethernet)
インターフェース	LAN 側	100BASE-TX/10BASE-T ×4 ポート
	WAN 側	100BASE-TX/10BASE-T ×1 ポート
		全ポート AUTOMDI/MDI-X 対応
	PCMCIA	TypeⅡ準拠(303/5V両対応)×1 ポート
ハードウェア構成	CPU	MIPS CORE
	メインメモリ	8MB
	フラッシュメモリ	1MB
電源仕様	ACアダプタ定格入力	AC100V(50/60Hz)
	定格出力	DC12V 1.0A
	最大消費電力	7.5W
環境条件	温度: 5 ～ 40℃ 湿度 25 ～ 85% 結露なきこと)	
重量	210g (ACアダプタ含まず)	
外計寸法	146(H) × 35(W) × 111(D)mm ＊付属品、突起部含まず	
サポートプロトコル	Ethernet	CSMA/CD
	ルーティング	IP のみ
	アドレス変換	NATP
	WAN	PPPoE 同時セッション 1
	認証	PAP
	ダイアルアップ	PPP
DHCP	サーバー(LAN 側最大 253 クライアント)	
	クライアント(WAN 側)	
アドレス変換	NAT/IP マスカレード	
VPN パススルー	IPsec、PPTP(1セッション)	
サーバー公開	バーチャルサーバー	
	DMZ ホスト	
アップグレード	WWW ブラウザによりアップグレード	
WakeOn 認証方式		メッセージ登録×1
		メッセージ認証 /CLID × 50 件
VOICEWakeOn 認証方式		着信番号登録× 50
		CLID × 50 件
リモートアクセス	プロトコル	PIAFS2.2/2.1/2.0/1.0/FOMA64K (モバイルカードに依存)
		着信番号登録× 50
	認証方式	CLID × 50 件、PAP 、CHAP
リモートアクセス :ファイアウォール		NAT 、IP フィルタ、バーチャルサーバー
アドレス解決	メールアカウント設定× 1	
	メール内容編集× 1	
プロトコル	SMTP 、POP	
	DNS サーバー選択	
運用サポート	通信ログ	
	WAN ハートビート	

外形寸法（単位 mm）　＊付属物・突起部含まず

◆ 資料1 ◆

遮断ログ

ファイアウォールが検出した不正なパケットの情報は「遮断ログ」に記録されます。
このログに表示されるパケットは Rooster が破棄するので、外部ネットワークにも内部ネットワークにも流れません。

Port Filter Defense

接続しようとしたポートはフィルタリングされています。
このポートを使ったアプリケーションを使用する場合は「高度な設定」の「フィルタリング」で設定をしてください。

Default Defense

ファイアウォールのデフォルト設定で接続が禁止されています。

Disallowed Destination IP

送信先の IP アドレスにはパケットを送信出来ません。

Invalid IP Packet Size

パケットヘッダのサイズが誤っています。

Black List Defense

送信元の IP アドレスはブラックリストに登録されています。ブラックリストは動的に作られます。

Invalid Configuration

NAT を使用する設定になっているにもかかわらず、グローバル ネーム スペースがありません。

No Existing Session

対応するセッションがありません。

No Enough Resources

Rooster のメモリ不足でセッションが確立できません。

◆ 資料 2 ◆

Rooster のファイアウォール機能

Rooster は以下のようなサービス拒否（DoS）攻撃やスキャンを検出してブロックするファイアウォール機能を持ちます。

サービス拒否（DoS）攻撃

SynFlood

大量の接続要求パケット（SYN パケット）を送信することで相手サーバに過剰な負荷をかけるサービス拒否（DoS）攻撃です。

andAttack

TCP 接続要求パケット（SYN パケット）を偽造して、送信元 IP アドレスとポート番号の両方を送信先と同一にするという方法で、相手サーバが無限ループに陥ることを狙ったサービス拒否（DoS）攻撃です。

LWinNuke

NETBIOS ポート（139）に帯域外通知（OOB）データを送ることで相手サーバをダウンさせようとする攻撃です。Windows 95 だけが影響を受けます。

Smurf

Ping パケットの送信元 IP アドレスを攻撃対象の IP アドレスに偽装して、ブロードキャストとして送信します。この結果、攻撃対象のサーバはネットワーク上のすべてのマシンから Ping 応答を受け取ることになり、過負荷状態に陥ります。

Boink

TCP/IP パケットのフラグメントオフセットを改竄して相手サーバが分割されたパケットを再構築する際に巨大すぎて扱えないようにするサービス拒否（DoS）攻撃です。

IcmpFlood

大量の ICMP パケットを送って、サーバやネットワークに過剰な負荷をかけるサービス拒否（DoS）攻撃です。

AscendKill

ASCEND 社ネットワーク機器は UDP ポート 9（Discard）を使ったリモートメンテナンス機能を持つ機種があります。この機能を悪用したサービス拒否（DoS）攻撃です。

EchoStorm

ICMP エコーサービスを悪用したサービス拒否（DoS）攻撃です。大量の ECHO パケットを送って相手サーバやネットワークに過剰な負荷をかけます。

Jolt

フラグメントされた巨大なパケットを受け取ると Windows95 がハングアップするという問題を悪用したサービス拒否（DoS）攻撃です。

OverDrop

Linux 2.0 のあるバージョンはフラグメントされたパケットを受け取ると IP モジュールのデバッグ用メッセージを出力するものがあります。このとき、巨大なパケットを受け取るとメモリフォルトを発生することがあります。この問題を悪用したサービス拒否（DoS）攻撃です。

PingOfDeath

規定サイズ以上の大きさの Ping パケットを送って、相手サーバをクラッシュさせるサービス拒否（DoS）攻撃です。

EchoChargen

ネットワークの動作や性能を目的に用意されている 2 つのサービスを組み合わせて、故意に大量のトラッフィックを発生させるサービス拒否（DoS）攻撃です。UDP パケットを偽装して、相手サーバの Chargen ポート向けに Echo ポートからのパケットを送ります。Chargen サービスはランダムな文字列を送信元に返すサービスなので、偽装された自身の Echo ポートに文字列を送信します。Echo サービスはその文字列をまた Charegen ポートに送り返すため無限ループとなり、過大な負荷が発生します。

ポートスキャン

ImapSynFinScan

IMAP ポートのスキャンです。古いバージョンの IMAP はセキュリティの脆弱性が報告されているのでそれを悪用したクラッキングを行おうとする者がスキャンをしている可能性があります。

UdpEchoScan

EchoChargen など UDP の Echo サービスを悪用しようとする者が UDP Echo ポートのスキャンを行っている可能性があります。

ChargenScan

EchoChargen など Chargen サービスを悪用しようとする者が Chargen ポートのスキャンを行っている可能性があります。

TcpSynAckScan

TCP パケットの SYN フラグを悪用したポートスキャンの手法です。ポートが開いているかを調べます。SYN を送って SYN/ACK が帰ってくるか、それとも RST/ACK が帰ってくるかをみることで、ポートの状態を知ります。

TcpFinScan

TCP パケットの FIN フラグを悪用したポートスキャンの手法です。ポートが開いているかを調べます。FIN を送って RST が帰ってくるかをみることで、ポートの状態を知ります。

TcpResetScan

全ての TCP フラグを "0" にするスキャン手法です。ポートが開いているかを調べます。FIN を送って RST が帰ってくるかをみることで、ポートの状態を知ります。

XmasTree

全ての TCP フラグを "1" にするスキャン手法です。ポートが開いているかを調べます。FIN を送って RST が帰ってくるかをみることで、ポートの状態を知ります。

BackOrificeScan

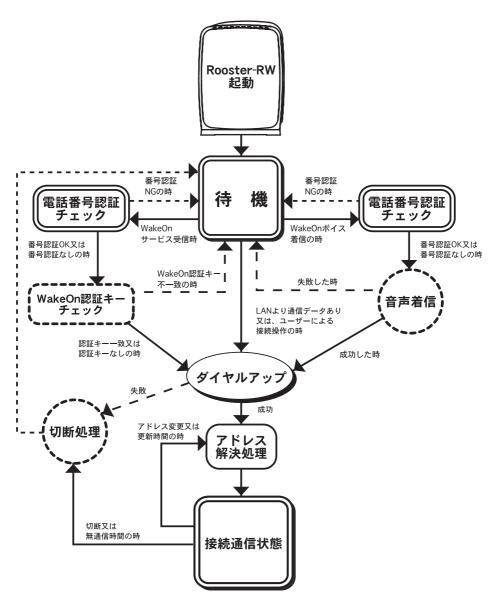
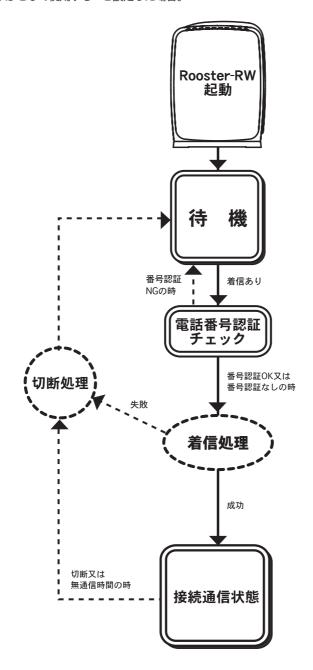
BACK ORIFICE（トロイの木馬）が仕掛けられていないかどうかを調べるスキャンです。

NetBusScan

Net Bus（トロイの木馬）が仕掛けられていないかどうかを調べるスキャンです。

◆ 資料３ ◆

モバイルカード動作フロー図

①“ダイヤルアップとして使用する”と設定した場合。

②“RAS として使用する ” と設定した場合。

サポートのご案内

最新情報の入手
本製品に関する最新情報は、インターネットのウェブページで入手することができます。また、
バージョンアップ情報もウェブページ上で公開していますので、ご活用下さい。

■本製品に関するウェブページ
http://www.sun-denshi.co.jp/sc/rooster-rw/
■本製品に関するFAQ
http://www.sun-denshi.co.jp/sc/rooster-rw/faq/
■本製品のバージョンアップ情報
http://www.sun-denshi.co.jp/sc/rooster-rw/verup/

ご質問・お問合せ
本製品に関するご質問やお問合せは、下記へご連絡下さい。

サン電子株式会社　サンコミュニケーションズ事業部　サポートセンター
電話　0587-55-0161
FAX　0587-55-0815
メール　support-suncomm@sun-denshi.co.jp
■受付時間　月～金曜日　10:00 ～ 16:00 （12:00 ～ 13:00 除く）
※祝祭日、当社の休日を除く

SC-RS5FJ
取扱説明書 Ver.1.2

サン電子株式会社　サンコミュニケーションズ事業部　2008 年 4 月発行
〒 483-8555　愛知県江南市古知野町朝日 250